Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

25/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Eléments de démonstration

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Il y a $\frac{\varphi(n)}{2}$ décompositions possibles qui font intervenir deux unités complémentaires.

On considère donc l'ensemble des unités à n, n étant un nombre pair supérieur ou égal à 6. On va démontrer que si tous les nombres premiers (forcément impairs) unités à n sont congrus à n selon un certain module, on aboutit à une contradiction. Cela aura pour conséquence que l'un des nombres premiers impairs inférieurs à n et premiers à n devant être incongru à n selon tout module premier impair inférieur à $\sqrt{n}$, ce nombre premier a son complémentaire à n qui est premier également. Le nombre premier en question est donc un décomposant de Goldbach de n.

Pour cela, on va utiliser trois éléments :

- les articles 129 page 95 et suivants des Recherches Arithmétiques : Théorème. *Si a est un nombre premier de la forme $8n+1$, il y aura nécessairement au-dessous de $2\sqrt{a}$ un nombre premier dont a est non-résidu.* ainsi que les articles suivants qui démontrent la Loi de Réciprocité Quadratique. Par exemple, dans l'article 131, *Tout nombre qui, pris positivement, est résidu ou non-résidu de p, aura pour résidu ou non-résidu, $+p$ ou $-p$, selon que p sera de la forme $4n+1$ ou $4n+3$.* Cela signifie entre les lignes que, modulo un certain nombre pair n, tous les nombres premiers unités de n ne peuvent être simultanément tous des résidus quadratiques de n ou bien tous des non-résidus quadratiques de n.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

- enfin, l'extrait de l'article 5 de la section 1 des Recherches : *"On doit supposer la même identité de module dans ce qui suit."*, et plus loin, dans l'article 7, *Si* $A \equiv a$ *et* $B \equiv b$, $AB \equiv ab$ (conservation des congruences par le produit).

Ecrivons comme hypothèse initiale que chaque nombre premier impair inversible est congru à n selon un module :

$$\begin{cases} p_1 \equiv n \ (mod\ p'_1) \\ p_2 \equiv n \ (mod\ p'_2) \\ \vdots \\ p_i \equiv n \ (mod\ p'_i) \end{cases}$$

Première remarque : les p'_i ne peuvent être des diviseurs de n ; en effet, d'une congruence de la forme $p_i \equiv n \ (mod\ p'_i)$, on tire une congruence de la forme $n - p_i \equiv 0 \ (mod\ p'_i)$. Mais pour que p'_i puisse être un diviseur de n tout en étant module d'une telle congruence, il faudrait que p'_i divise également p_i ce qui est impossible.

Si l'on s'intéresse à deux congruences faisant intervenir respectivement les nombres premiers p_u et p'_u d'une part, et les nombres premiers p_v et p'_v d'autre part, on se trouve alors face à deux cas de figure :

- soit, sous prétexte que les p'_i ne sont jamais des diviseurs de n et qu'ils sont donc en nombre moindre que les p_i, on a une redondance des deux modules qui s'avèrent égaux $p'_u = p'_v$. Les deux congruences :

  $$\begin{cases} p_u \equiv n \ (mod\ p'_u) \\ p_v \equiv n \ (mod\ p'_v) \end{cases}$$

  se transforment en une seule

  $$p_u.p_v \equiv n^2 \ (mod\ p'_u)$$

  qui est une congruence quadratique, et nous amène à conclure que soit et p_u et p_v sont deux résidus quadratiques de n, soit et p_u et p_v sont deux non-résidus quadratiques de n (seul le produit de deux résidus ou de deux non-résidus quadratiques peut être congru à un carré) ;

- soit, on a à affaire à deux congruences de modules différents :

  $$\begin{cases} p_u \equiv n \ (mod\ p'_u) \\ p_v \equiv n \ (mod\ p'_v) \end{cases}$$

  Et là, on ne sait pas quoi faire pour se ramener à une congruence quadratique, qui nous permettrait par exemple de proche en proche d'aboutir à une contradiction sous-prétexte que tous les nombres premiers s'avèreraient être des résidus quadratiques seulement ou bien des non-résidus quadratiques seulement, ce qui est impossible.

  Donc on ne peut toujours pas dire qu'il existe un nombre premier incongru à n selon tout nombre premier impair inférieur à $\sqrt{n}$ et qui fournit une décomposition de Goldbach de n.